



W H I T E P A P E R

**Kaspersky Anti-Virus für  
Windows Server  
Enterprise Edition**



Im immer rauerem Wettbewerbsklima müssen sich Firmen durch effiziente Strategien und optimierte Prozesse behaupten. Grundvoraussetzungen, die dafür an die IT-Systeme gestellt werden, sind eine hohe Sicherheit und ständige Verfügbarkeit der Daten. Kaspersky Labs rät deshalb zu einem mehrstufigen Schutzsystem, das nicht nur die Clients der Mitarbeiter schützt, sondern auch Server und Gateways miteinbezieht. Besonders wichtig ist der Virenschutz für die eingesetzten File-Server, da eine einzige infizierte Datei auf dem Server zur Infektions-Quelle für alle Anwender-PCs werden kann, die auf diese Ressource zugreifen. Ein zuverlässiger Schutz des Datei-Servers gewährleistet aber nicht nur die sichere Arbeit der Anwender sowie die Integrität der Daten, sondern verhindert auch die Infektion von Backup-Dateien, so dass wiederholte Virus-Epidemien ausgeschlossen werden.

Zu diesem Zweck bietet Kaspersky Labs eine für den Einsatz auf File-Servern optimierte Version seiner bewährte Antiviren-Lösung an: Kaspersky Anti-Virus für File-Server. Hinter dieser Produktbezeichnung stehen wiederum Einzellösungen für verschiedene Betriebssysteme:

- ▶ **Microsoft Windows:**  
Kaspersky Anti-Virus für Windows Server
- ▶ **Linux:**  
Kaspersky Anti-Virus für Linux File Server
- ▶ **Novell Netware:**  
Kaspersky Anti-Virus für Novell Netware
- ▶ **Samba:**  
Kaspersky Anti-Virus für Samba Server

Für die immer höheren Anforderungen im Storage-Bereich gibt es nun zusätzlich das neue Kaspersky Anti-Virus für Windows Server Enterprise Edition. Dieses schützt Terminal-Server von Microsoft sowie Citrix und bietet auch Support für Windows-Server im Cluster-Betrieb sowie für den Windows Storage Server.

In diesem Whitepaper liegt der Fokus auf Kaspersky Anti-Virus für Windows Server und der neuen Kaspersky Anti-Virus für Windows Server Enterprise Edition.

### Kurz & bündig

Infizierte Dateien auf einem File-Server, der Arbeitsgruppen oder gar ganzen Firmen zur Zusammenarbeit dient, können im Handumdrehen alle angeschlossenen Clients im Netzwerk infizieren. Um diese Epidemie zu verhindern, empfiehlt Kaspersky den gezielten Schutz von Datei-Servern in Echtzeit. Speziell für Windows File-Server gibt es zwei Produkte:

- ▶ Kaspersky Anti-Virus für File-Server
- ▶ Kaspersky Anti-Virus für Windows Server Enterprise Edition

Die Enterprise Edition enthält einige erweiterte Funktionen für Großunternehmen, etwa Support für Citrix und Microsoft Terminal Server sowie SAN-Unterstützung. In beiden Systemen sucht die mehrfach ausgezeichnete Kaspersky-Scan-Engine mit hervorragenden Erkennungsraten nach Schädlingen. Die File-Server werden permanent überwacht und können auch manuell oder zeitgesteuert durchsucht werden.

Clever gelöst sind die Funktionen zum Sparen von Rechenpower: So werden alle Objekte anfangs nur einmal gescannt und bei Folgedurchläufen nur dann erneut geprüft, wenn sie verändert wurden. Dateien, die auf dem File-Server und auf Clients mit Kaspersky Anti-Virus doppelt vorkommen, werden nur auf dem Server auf Viren geprüft. Findet das Antiviren-Programm Schädlinge, dann entfernt es sie und stellt die sauberen Daten wieder her. Viren können gelöscht oder unter Quarantäne gestellt werden.

Um die Arbeit der angeschlossenen Clients nicht zu stören, können Administratoren den File-Server-Schutz flexibel anpassen und etwa eine maximale Zahl von Prozessen definieren oder bei Servern mit mehreren CPUs die Antiviren-Prozesse geschickt verteilen. Vertrauenswürdige Prozesse wie ein Defragmentierer können ganz vom Scan befreit werden. Für einzelne Ordner oder Laufwerke merkt sich Kaspersky auf Wunsch auch eigene Scan-Parameter. Da sich diese Einstellungen als Vorlagen speichern und auf andere Objekte übertragen lassen, sparen Administratoren Zeit.

Die Administration läuft remote von der Workstation des Administrators aus, beide Programme bringen das Kaspersky Administration Kit mit. Die Enterprise Edition hat auch noch ein Snap-in für die Management Console integriert und bietet wahlweise auch eine Kommandozeilenfunktion an. Damit steuert man den Virenschanner komplett über das Netzwerk und wertet auch bequem die umfangreichen Report-Daten aus.

### Zusatzfeatures der Enterprise Edition

Für den Schutz von Windows-Datei-Servern hat Kaspersky zwei Versionen im Angebot: Kaspersky Anti-Virus für File-Server und Kaspersky Anti-Virus für Windows Server Enterprise Edition. In der folgenden Liste sind die erweiterten Funktionen der Enterprise Edition zusammengestellt:

- ▶ **Schutz für Terminal Server**  
Die Enterprise Version läuft auch auf Microsoft Terminal Servern, Citrix Metaframe XPe FR3 und Citrix Presentation Server; dabei wird die Veröffentlichung von Arbeitsplätzen und Anwendungen unterstützt.
- ▶ **Support für Cluster**  
Der Virenschutz funktioniert auf allen Knoten-Rechnern eines Windows-Clusters; beim Ausfall von Knoten arbeitet der Virenschanner auch beim und nach dem Failover einwandfrei weiter.

- ▶ **Individuelle Schutzparameter für bestimmte Bereiche**  
Festgelegte Bereiche wie einzelne Ordner oder ganze Laufwerke können mit individuellen Schutzeinstellungen versehen werden.
- ▶ **Parametervorlagen**  
Festgelegte Einstellungen für einzelne Schutzbereiche können als Vorlagen gespeichert werden.
- ▶ **Aktion für ein Objekt in Abhängigkeit vom Typ der gefundenen Bedrohung ausführen**  
Desinfizieren, in Quarantäne schicken oder Löschen – das geht jetzt auch gezielt in Abhängigkeit vom Bedrohungstyp wie Virus oder Trojaner.
- ▶ **Sperren des Zugriffs auf einen Server mit infizierten Elementen**  
Administratoren können den Zugriff für Workstations auf einen Server mit infizierten Objekten automatisch für eine festgelegte Zeit sperren.
- ▶ **Skript-Untersuchung**  
Der Virens Scanner prüft auch ausführbare Skripts auf Schädlinge.
- ▶ **Unterstützung von SNMP**  
Der aktuelle Schutzstatus wird per SNMP (Simple Network Management Protocol) gemeldet und kann so automatisiert überwacht werden.
- ▶ **Speichern von Zugriffsrechten für Dateien und Ordner beim Verschieben in die Quarantäne oder in das Backup**  
Meta-Informationen wie Besitz- und Zugriffsrechte bleiben auch dann erhalten, wenn der Virens Scanner eine Datei in Quarantäne verschiebt.
- ▶ **Verwaltung über MMC**  
Ein mitgeliefertes Snap-in erlaubt die Verwaltung über Microsofts Management Console; alternativ ist auch die Steuerung per Kaspersky Administration Kit oder Kommandozeile möglich.
- ▶ **SAN-Unterstützung (Windows Storage Server)**  
Mit dem Support für Windows Storage Server schützt Kaspersky Anti-Virus für Windows Server Enterprise Edition auch die Dateien in einem Storage Area Network.

## Hauptvorteile

Kaspersky Anti-Virus für Windows Server schützt die gemeinsam genutzten Datenspeicher in Echtzeit. Das neueste Produkt Kaspersky Anti-Virus für Windows Server Enterprise Edition wartet mit einigen zusätzlichen Highlights auf: Die Software ist für den Einsatz auf Citrix und Microsoft Terminal Server zertifiziert. So wird das Einsatzspektrum vom File-Server auf Terminal- und Anwendungs-Server erweitert. Außerdem ist es möglich, diese Version von Kaspersky Anti-Virus auf Servern zu betreiben, die als Domänen-Controller arbeiten.

Ein weiterer Vorteil: Die Enterprise-Version unterstützt auch den Windows-Cluster-Betrieb. So läuft eine In-

stanz des Virens Scanners auf jedem Knoten. Fällt ein Knoten aus, harmonisiert Kaspersky Anti-Virus auch mit dem dann einsetzenden Failover des Clusters. Um den Virenschutz fit für den Einsatz in Storage Area Networks (SAN) zu machen, unterstützt Kaspersky Anti-Virus für Windows Server Enterprise Edition auch den Windows Storage Server.

## Gemeinsame Daten optimal schützen

Mit Kaspersky Anti-Virus für File-Server besitzen Sie einen Echtzeit-Virenschutz. Das Schutz-Programm überprüft alle gestarteten, geöffneten sowie veränderten Dateien auf Schädlingsbefall. Werden Viren oder andere Bedrohungen entdeckt, repariert oder entfernt die Software infizierte Objekte und isoliert verdächtige Komponenten in einem eigenen Quarantäne-Ordner zur weiteren Analyse. Ein besonderes Features der Enterprise Edition: Metainformationen für die verschobenen Dateien wie Zugriffsrechte bleiben dabei erhalten.

Kritische System-Bereiche wie die Autostart-Einträge prüft ein spezielles Modul, ebenso werden ausführbare Skripts untersucht. So lassen sich etwa getarnte Prozesse von Rootkits erkennen. Um Virus-Epidemien zu vermeiden, beobachtet die Software stets die aktuelle Viren-Aktivität und bemerkt frühzeitig Virus-Attacken. So können Administratoren frühzeitig reagieren, sei es durch manuelle Prüfung, Datenbank-Updates oder Anpassung der Sicherheits-Stufe. Infizierten Workstations kann der Administrator den Zugriff auf den File-Server für eine bestimmte Zeit verbieten. Der Vorteil: Die potenzielle Infektionsquelle kann in der Zwischenzeit gesäubert werden.

Nach dem Entfernen von Schädlingen löscht der Virens Scanner auch sämtliche durch dieses Objekt erstellten Einträge in den System-Dateien und in der Registry. Dadurch werden Folgeinfektionen und Systemausfälle wirksam verhindert.

## Höchstleistung mit wenig Ressourcen

Besonders gut skaliert Kaspersky Anti-Virus auf File-Servern mit mehreren Prozessoren. Der Administrator bestimmt dabei die maximale Anzahl der aktiven Antiviren-Prozesse oder legt gezielt fest, welche CPU für die Aufgaben des Antiviren-Programms zuständig ist. Die Verteilung der Server-Ressourcen zwischen dem Antiviren-Programm und anderen Anwendungen wird automatisch reguliert – abhängig von der Priorität der Aufgaben. Beim ersten System-Scan checkt Kaspersky Anti-Virus alle Objekte, bei nachfolgenden Prüfungen werden nur die neuen und veränderten Daten kontrolliert – das spart Zeit und Rechenpower.

Dateien, die sowohl auf dem File-Server als auch auf der Workstation vorhanden sind, werden nur auf dem Server geprüft, wenn Kaspersky Anti-Virus auch auf dem Client läuft. Zusätzlich erhöht sich die Scan-

Geschwindigkeit, wenn der Administrator ungefährliche Prozesse wie etwa Backup-Jobs von der Prüfung ausschließt. Um die Server-Ressourcen optimal zu nutzen und das Arbeiten für die angeschlossenen Clients so komfortabel wie möglich zu machen, können Start und Ende von Routine-Scans frei definiert werden. Die Virenprüfung läuft also etwa dann ab, wenn der Server minimal belastet ist – beispielsweise nachts.

### Flexible Administration

Kaspersky Labs gibt Administratoren leistungsfähige Werkzeuge für die Remote-Verwaltung des Virenschanners an die Hand. Das kostenlos erhältliche Kaspersky Administration Kit ermöglicht die entfernte Installation und zentrale Konfiguration des Programms auf mehreren Datei-Servern gleichzeitig. Auf einen Blick kann der Administrator den Schutzstatus des Netzwerks erkennen und einzelne Bereiche kontrollieren. Bei der Enterprise Version wird zusätzlich noch ein Snap-in für die Microsoft Management Console (MMC) mitgeliefert. Die Installation nehmen Administratoren einfach über Gruppenrichtlinien im Active Directory vor oder rufen das Installerpaket über die Kommandozeile auf. Das Schutzprogramm bietet außerdem die Möglichkeit, für verschiedene Bereiche wie Laufwerke oder Ordner auch unterschiedliche Scan-Parameter einzustellen. Einmal gemachte Einstellungen für einen Bereich lassen sich als Vorlage speichern und dann zeitsparend auf andere Objekte übertragen. Abhängig vom Typ der gefundenen Bedrohung kann der Virenschanner unterschiedlich reagieren, etwa Viren desinfizieren und Trojaner in Quarantäne schicken oder löschen.

### Updates schnell und unkompliziert

Die wichtigste Voraussetzung für einen gut funktionierenden Virenschanner ist eine stets aktuelle Antiviren-Datenbank. Kaspersky liefert stündlich neue Viren-Signaturen aus, die der Administrator automatisch oder nach einem individuellen Zeitplan einspielen kann. Als Update-Quellen funktionieren Kaspersky-Lab-Server oder festgelegte lokale Server. Das Antiviren-Programm wählt dabei selbständig den am wenigsten belasteten Update-Server aus.

### Bedrohungslage im Blick

Administratoren sind mit dem umfangreichen Berichtssystem stets im Bilde, wie es um den Virenschutz der IT-Systeme steht. Die Software erstellt anschauliche Berichte über die Arbeit des Programms sowie den Schutzstatus – entweder im HTML-Format, als Windows-Ereignis-Protokoll oder als Protokoll des Kaspersky Administration Kits. Die Erstellungsintervalle und Inhalte der Berichte können individuell bestimmt werden. Kaspersky Anti-Virus für Windows Server

## Systemanforderungen

**Kaspersky Anti-Virus für Windows Server:**

**Festplattenspeicher:** 50 MByte frei

**Sonstiges:** Microsoft Windows Installer 2.0, Microsoft Internet Explorer 5.5 oder höher

**Unterstützte Betriebssysteme:** Microsoft Windows 2000 Server/Advanced Server Service Pack 4 oder höher, alle Aktualisierungen, Microsoft Windows NT Server 4.0 Service Pack 6a, Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, alle Service Packs, alle Aktualisierungen, Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition

**Kaspersky Anti-Virus für Windows Server Enterprise Edition:**

**Festplattenspeicher:** 70 MByte frei, 400 MByte zum Speichern von Objekten in Quarantäne und Backup, 100 MByte zum Speichern von Berichten

**Minimalkonfiguration:** Prozessor Intel Pentium II mit 400 MHz und höher, 256 MByte RAM

**Empfohlene Konfiguration:** Prozessor Intel Xeon mit 3,2 GHz oder höher, 1 bis 2 GByte RAM

**Sonstiges:** Microsoft Windows Installer 3.1, Microsoft Internet Explorer 5.5 oder höher

**Unterstützte Betriebssysteme:** Microsoft Windows Server 2003 x64 Standard Edition, Microsoft Windows Server 2003 x64 Enterprise Edition, Microsoft Windows Server 2003 x64 Datacenter Edition, Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Datacenter x64 Edition, Microsoft Windows 2000 Server mit Service Pack 4 + Rollup 1, Microsoft Windows 2000 Advanced Server mit Service Pack 4 + Rollup 1, Microsoft Windows Server 2003 Standard Edition mit Service Pack 1 oder höher, Microsoft Windows Server 2003 Enterprise Edition mit Service Pack 1 oder höher, Microsoft Windows Server 2003 Datacenter Edition mit Service Pack 1 oder höher, Microsoft Windows Server 2003 R2 Standard Edition oder höher, Microsoft Windows Server 2003 R2 Enterprise Edition oder höher, Microsoft Windows Server 2003 R2 Datacenter Edition oder höher, Microsoft Windows Storage Server 2003 R2 oder höher

Enterprise Edition erlaubt das Speichern und Bearbeiten einer großen Anzahl von Berichtseinträgen und Quarantäne-Backup-Objekten. Eine leistungsfähige Suche sowie ein ausgefeiltes Filtersystem sind ebenfalls enthalten. Ein weiteres Plus: Per SNMP-Schnittstelle können Administratoren den Sicherheitsstatus der File-Server nahtlos in ein bestehendes Monitoring-System integrieren.

## Lizenzierung

Zum Einsatz des Programms ist ein gültiger Lizenzschlüssel nötig (eine einfache Textdatei mit der Endung *.key*). Dieser Schlüssel legt genau fest, welche Einschränkungen und Berechtigungen beim Einsatz von Kaspersky Anti-Virus für Windows Server gelten. Beachten Sie bitte, dass nach Ablauf des Schlüssels der Virenschutz für Ihre Systeme nicht mehr gewährleistet werden kann, weil die Updates nicht mehr eingespielt werden.

Um nicht aus Versehen das Auslaufen des Keys zu übersehen, gibt es die Möglichkeit, für das Programm gleichzeitig zwei Schlüssel zu installieren: Ein Schlüssel ist aktiv, der andere Schlüssel dient als Notreserve und springt sofort ein, wenn die Gültigkeit des aktiven Schlüssels abgelaufen ist.

Der Lizenzbedarf für Kaspersky Anti-Virus für Windows Server richtet sich nicht nach der Anzahl der angeschlossenen Nodes. Für Fragen zur Lizenzierung wenden Sie sich bitte an [vertrieb@kaspersky.de](mailto:vertrieb@kaspersky.de).

## Installation & Deployment

Entfernen Sie vor der Installation von Kaspersky Anti-Virus für File-Server unbedingt alle anderen Virens Scanner vom Datei-Server. Verschiedene Virens Scanner auf einem System können zu unerwünschten Wechselwirkungen führen. Jedoch harmoniert der File-Server-Schutz hervorragend mit Kaspersky Anti-Virus für Desktop-PCs.

Der Virenschutz wird direkt auf dem File-Server installiert, die Konfigurations-Software liefert Kaspersky Labs bei Anti-Virus für Windows Server Enterprise Edition als Plug-in für die Microsoft Management Console (MMC) mit. Sie wird im Normalfall auf der Workstation des Administrators installiert. Alternativ ist auch die Installation via Kommandozeile beim Enterprise-Produkt möglich. Alle anderen Kaspersky-Lösungen für File-Server werden über das beiliegende Kaspersky Administration Kit verwaltet. Dieses läuft ebenfalls auf dem Rechner des Admins und verwaltet den File-Server-Schutz remote.

Im Installationspaket enthält die Enterprise Edition Ordner für 32-Bit- und 64-Bit-Systeme. Im Unterordner server liegen die Kernkomponenten für die Installation auf dem File-Server, im Ordner client dagegen die nötigen Files für die MMC.

Kaspersky empfiehlt für die Installation drei Schritte:

- 1 **Wählen Sie die Administrationswerkzeuge:**  
Sie haben die Wahl zwischen MMC, Kommandozeile und Kaspersky Administration Kit.
- 2 **Bestimmen Sie die nötigen Programm-Komponenten:**  
Nicht alle Komponenten sind auf jedem Server nötig. Wählen Sie die passenden Module für Ihre Umgebung aus.
- 3 **Entscheiden Sie sich für eine Installationsmethode:**  
Abhängig von Ihrer Netzwerk-Architektur können Sie die Installationsmethode wählen. Hier können Sie spezielle Parameter verwenden. Sie können Kaspersky Anti-Virus sowohl mit dem Installationsassistenten als auch durch Start der Installer-Datei (*.msi*) des Installationspakets aus der Befehlszeile installieren. Außerdem können Sie Kaspersky Anti-Virus zentral als Remote-Installation über Gruppenrichtlinien des Active Directory oder mit der Aufgabe zur Remote-Installation vom Kaspersky Administration Kit aus installieren.

## Fazit

Gegen aktuelle IT-Bedrohungen besteht der beste Schutz aus mehreren Stufen. Deshalb sollten Firmen zusätzlich zum Client- und Server-Schutz ihre Internet-Gateways mit Antiviren-Software ausstatten. Ein gefährlicher Infektionsherd sind File-Server, auf die komplette Firmen oder Teams zugreifen. Ein Virenschutz für File-Server ist deshalb unbedingt anzuraten.

Kaspersky Anti-Virus für File-Server ist solch eine Schutz-Software, die speziell für den Einsatz auf File-Servern optimiert ist. First-Class-Security ist dabei gepaart mit zentraler Verwaltung und niedrigem Ressourcen-Verbrauch. Um den Schutz auch auf SANs, Cluster sowie Citrix und Microsoft Terminal Server auszuweiten, hat Kaspersky Labs das neue Produkt Kaspersky Anti-Virus für Windows Server Enterprise Edition im Programm.

Besonderheiten sind ein mitgeliefertes MMC-Snap-in, eine SNMP-Schnittstelle, individuelle Schutzparameter für bestimmte Bereiche, Parametervorlagen und die automatische Zugriffssperre auf File-Server mit infizierten Dateien.

Updates sind schnell und unkompliziert via Internet oder lokalem Update-Server eingespielt. Die eingebauten Reporting-Funktionen geben jederzeit Überblick über den aktuellen Stand der Schutz-Systeme.

## Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crime-ware, Hacker, Phishing-Attacken und Spam.

Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht.

Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

### Kontakt

Kaspersky Labs GmbH  
Steinheilstr. 13  
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0  
Telefax: +49 (0)841 981 89 100

[www.kaspersky.de](http://www.kaspersky.de)